Abstract

Cryptographic method and apparatus for non-linearly merging a data block and a key

The method and apparatus are used for cryptographically converting a digital input block into a digital output block. The apparatus 400 comprises first input means 410 for obtaining the digital input block and second input means 440 for obtaining a key K1. Cryptographic processing means 420 of the apparatus 400 convert the digital input block into the digital output block by merging a selected part M1 of the digital input block with the key K1 and producing a data block B1 which non-linearly depends on M1 and K1. The merging is performed in one, sequentially inseparable step. Output means 430 are used to output the digital output block of which a selected part is derived from B1.

Fig. 6.